09/807607

2121

Copie à l'intention de l'office élu (EO/US)

PCT/FR99/02172

TRAITÉ DE COOPERATION EN MATIÈRE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Destinataire:

NONNENMACHER, Bernard
Gemplus
Avenue Du Pic De Bertagne
Parc D'activités De Gémenos
F-13881 Gémenos Cedex
FRANCE

Date d'expédition (jour/mois/année)
01 novembre 2001 (01.11.01)

Référence du dossier du déposant ou du mandataire
GEM 587

NOTIFICATION IMPORTANTE

Demande internationale no
PCT/FR99/02172

Date du dépôt international (jour/mois/année)
13 septembre 1999 (13.09.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:
☐ le déposant ☐ l'inventeur ☒ le mandataire ☐ le représentant commun

Nom et adresse
CABINET BALLOT
4, rue Général Hoche
F-56100 Lorient
FRANCE

Nationalité (nom de l'Etat)

Domicile (nom de l'Etat)

no de téléphone
02.97.21.87.87

no de télécopieur
02.97.64.55.77

no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:
☒ la personne ☐ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse
NONNENMACHER, Bernard
Gemplus
Avenue Du Pic De Bertagne
Parc D'activités De Gémenos
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat)

Domicile (nom de l'Etat)

no de téléphone
04.42.36.63.56

no de télécopieur
04.42.36.63.43

no de téléimprimeur

3. Observations complémentaires, le cas échéant:
Ce formulaire remplace le formulaire IB/306 du 10 août 2001 fait par erreur.

4. Une copie de cette notification a été envoyée:
☒ à l'office récepteur
☐ à l'administration chargée de la recherche internationale
☐ à l'administration chargée de l'examen préliminaire international
☐ aux offices désignés concernés
☒ aux offices élus concernés
☒ autre destinataire: CABINET BALLOT

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:
Sean Taylor

no de téléphone (41-22) 338.83.38

Formulaire PCT/IB/306 (mars 1994)

004421149

Copie à l'intention de l'office élu (EO/US) PCT/FR99/02172

09/807607

TRAITÉ DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Destinataire:

CABINET BALLOT
4, rue Général Hoche
F-56100 Lorient
FRANCE

RECEIVED
SEP 19 2001
Technology Center 2100

Date d'expédition (jour/mois/année)	
10 août 2001 (10.08.01)	
Référence du dossier du déposant ou du mandataire GEM 587	**NOTIFICATION IMPORTANTE**
Demande internationale no PCT/FR99/02172	**Date du dépôt international** (jour/mois/année) 13 septembre 1999 (13.09.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☐ le déposant ☐ l'inventeur ☒ le mandataire ☐ le représentant commun

Nom et adresse	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)
NONNENMACHER, Bernard Gemplus Avenue du Pic de Bertagne Parc d'activités de Gémenos F-13881 Gémenos Cedex FRANCE		

no de téléphone 04-42-36-63-56
no de télécopieur 04-42-36-63-43
no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☒ la personne ☐ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)
CABINET BALLOT 4, rue Général Hoche F-56100 Lorient FRANCE		

no de téléphone 02.97.21.87.87
no de télécopieur 02.97.64.55.77
no de téléimprimeur

3. Observations complémentaires, le cas échéant:

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur
☐ à l'administration chargée de la recherche internationale
☐ à l'administration chargée de l'examen préliminaire international
☐ aux offices désignés concernés
☒ aux offices élus concernés
☒ autre destinataire: NONNENMACHER, Bernard

Bureau international de l'OMPI **34, chemin des Colombettes** **1211 Genève 20, Suisse**	Fonctionnaire autorisé: Sean Taylor
no de télécopieur (41-22) 740.14.35	no de téléphone (41-22) 338.83.38

Formulaire PCT/IB/306 (mars 1994) 004205409

Copie à l'intention de l'office élu (EO/US) PCT/FR99/02172

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Destinataire:

NONNENMACHER, Bernard
Gemplus
Avenue du Pic de Bertagne
Parc d'activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Date d'expédition (jour/mois/année)
03 octobre 2000 (03.10.00)

Référence du dossier du déposant ou du mandataire
GEM 587

NOTIFICATION IMPORTANTE

Demande internationale no
PCT/FR99/02172

Date du dépôt international (jour/mois/année)
13 septembre 1999 (13.09.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

[X] le déposant [ ] l'inventeur [ ] le mandataire [ ] le représentant commun

Nom et adresse
GEMPLUS S.C.A.
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat): FR
Domicile (nom de l'Etat): FR
no de téléphone:
no de télécopieur:
no de téléimprimeur:

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

[ ] la personne [X] le nom [ ] l'adresse [ ] la nationalité [ ] le domicile

Nom et adresse
GEMPLUS
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat): FR
Domicile (nom de l'Etat): FR
no de téléphone:
no de télécopieur:
no de téléimprimeur:

3. Observations complémentaires, le cas échéant:

4. Une copie de cette notification a été envoyée:

[X] à l'office récepteur
[ ] à l'administration chargée de la recherche internationale
[X] à l'administration chargée de l'examen préliminaire international
[ ] aux offices désignés concernés
[X] aux offices élus concernés
[ ] autre destinataire:

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:
Dominique DELMAS

no de téléphone (41-22) 338.83.38

Formulaire PCT/IB/306 (mars 1994)

003559309

TRAITE [illegible] COOPERATION EN MATI[illegible] DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 09 juin 2000 (09.06.00)	
Demande internationale no PCT/FR99/02172	**Référence du dossier du déposant ou du mandataire** GEM 587
Date du dépôt international (jour/mois/année) 13 septembre 1999 (13.09.99)	**Date de priorité** (jour/mois/année) 16 octobre 1998 (16.10.98)
Déposant CLAVIER, Christophe etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

15 mai 2000 (15.05.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Diana Nissen

no de téléphone: (41-22) 338.83.38

A.P.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 587	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 99/ 02172	Date du dépôt international *(jour/mois/année)* 13/09/1999	(Date de priorité (la plus ancienne) *(jour/mois/année)* 16/10/1998
Déposant GEMPLUS S.C.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 1

   [X] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/02172

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997 (1997-11-03), pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS abrégé colonne 1, ligne 13 - ligne 29 colonne 2, ligne 6 - ligne 18 colonne 3, ligne 1 -colonne 5, ligne 1 --- -/--	1,2,10

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 janvier 2000	18/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

3

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THECONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 juillet 1994 (1994-07-01), pages 85-90, XP000460342 le document en entier	1
A	FR 2 672 402 A (GEMPLUS CARD INT) 7 août 1992 (1992-08-07) abrégé page 1, ligne 4 - ligne 12 page 3, ligne 19 - ligne 23 figure 1 revendication 1	11,12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 99/02172

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2672402 A	07-08-1992	NONE	

7
T

TRAITE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 587	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR99/02172	Date du dépot international *(jour/mois/année)* 13/09/1999	Date de priorité *(jour/mois/année)* 16/10/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/06		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 9 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 4 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
15/05/2000	24.01.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Agreda Labrador, A N° de téléphone +49 89 2399 8263

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02172

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).*) :

Description, pages:

1-22 version initiale

Revendications, N°:

1-12 reçue(s) avec télécopie du 16/10/2000

Dessins, feuilles:

1/8-8/8 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☐ des revendications, nos :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-12
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-12
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-12
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Il est fait référence aux documents suivants, cités dans le Rapport de Recherche Internationale:

D1: YI X ET AL: 'A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES' IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997, pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

D2: MIYAGUCHI S: 'SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY' NTT REVIEW, vol. 6, no. 4, 1 juillet 1994, pages 85-90, XP000460342

D3: FR-A-2 672 402 (GEMPLUS CARD INT) 7 août 1992

Concernant le point V: Déclaration motivée selon l'article 35.(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. La présente demande concerne un procédé (revendication 1) de contre-mesure dans un composant électronique mettant en ouvre un algorithme cryptographique à clé secrète (DES) pour calculer un message chiffré à partir d'un message d'entrée.

   Elle concerne aussi un composant électronique (revendication 11) et une carte à puce (revendication 12) mettant en oeuvre le procédé de contre-mesure.

   Ces algorithmes sont vulnérables à des attaques consistant en une analyse différentielle de consommation en courant (DPA). Les caractéristiques des algorithmes sont connues et certaines données calculées dépendent seulement du message appliqué en clair en entrée de la carte et de la clé secrète contenue dans la carte. Normalement, à chaque bit d'une donnée particulière correspond une sous-clé formée par un groupe particulier de bits de la clé. L'idée de base de l'attaque DPA est d'utiliser la différence du profil de consommation en courant d'une instruction, selon qu'elle manipule un 0 ou un 1 et la possibilité de calculer un bit cible (bit qui peut être prédit) à partir d'un message connu d'entrée ou de sortie et d'une hypothèse sur la sous-clé correspondante.

La présente invention a pour but de mettre en oeuvre dans un composant électronique, un procédé de contre-mesure qui entraîne un signal DPA nul, même dans le cas où l'hypothèse de sous-clé serait juste. Elle permet de rendre imprédictibles les bits cibles en faisant que un bit cible prend la valeur 1 ou 0 avec une égale probabilité.

En effet la solution de l'invention consiste à introduire dans certains tours de l'algorithme une séquence d'exécution alternative dont les résultats en sortie du dernier tour sont les mêmes que les résultats de la séquence originelle et dont les bits des données qui peuvent être prédits complémentent ceux de la séquence originelle.

2. Aucun des documents cités dans le Rapport de Recherche Internationale ne décrit un procédé de contre-mesure dans un composant électronique contre des attaques consistant en une analyse différentielle de consommation en courant:

- D1 décrit une méthode pour développer facilement et efficacement par ordinateur des boîtes-S (boîtes de substitution) fortes. Le DES pourrait être cassé si des boîtes-S pauvres étaient utilisées. Les boîtes inverses sont également fortes. La méthode possède une bonne propriété contre l'attaque différentielle.

- D2 se réfère à un algorithme principal secret de chiffrement qui change dynamiquement sous la commande de la clé de chiffrement. La méthode est résistante contre les attaques qui calculent la clé en utilisant des paires de texte en clair et de leur bloc de texte chiffré. Il contient un exemple avec un chiffre modifié de DES.

- D3 concerne un procédé et dispositif pour la génération de nombres pseudo-aléatoires uniques en utilisant l'algorithme DES qui s'applique à la réalisation de cartes à puces.

3. Une telle solution n'est donc ni décrite, ni dérivable des documents cités et une activité inventive est reconnue. En conséquence, les revendications 1, 11 et 12 remplissent les exigences de l'Article 33 PCT.

4. Les revendications 2-10 dépendent de la revendication 1 et satisfont donc également, en tant que telles, aux conditions requises par l'Article 33 PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VII: Irrégularités dans la demande internationale

1. En vue de remplir les conditions énoncées à la Règle 5.1(a)(ii) PCT, le Demandeur aurait dû citer dans la description les documents D1-D3 ou autres documents représentant l'état de la technique tel qu'il décrit à l'introduction de la description (pages 1-8 et 11-15) et aurait dû indiquer l'état correspondant de la technique. Il aurait dû aussi identifier ces documents conformément à la Règle 5.1(a)(ii) PCT.

2. En vue de remplir les conditions énoncées à la Règle 5.1(a)(iii) PCT, la partie introductive de la description aurait dû être mise en conformité avec les nouvelles revendications proposées par le Demandeur.

3. Le Demandeur pourrait avoir saisi l'occasion de ces amendements pour corriger des erreurs de frappe dans la demande:

- "constante" (page 16, ligne 2) devrait être "constantes".

Concernant le point VIII: Observations relatives à la demande internationale

1. En ce qui concerne les revendications indépendantes:

1a. La formulation "... prévoit l'utilisation d'autres moyens (TC1)... **en sorte que** la donnée de sortie et les données dérivées soient imprédictibles" utilisée dans la revendication 1 tente de **définir l'invention par le résultat recherché**.

Une telle formulation n'est pas suffisante (voir à ce propos les Directives PCT C-III-4.7 qui précisent que les revendications tentant de définir l'invention par le

résultat recherché ne sont pas autorisées) car elles ne contiennent pas toutes les caractéristiques essentielles nécessaires à la définition de l'invention (Article 6 en combinaison avec la Règle 6.3(b) PCT). En effet ce sont plutôt les caractéristiques définissant **quels sont ces moyens et comment lesdits moyens sont agencés, connectés et utilisés**, afin de permettre d'arriver à ce résultat, que l'on devrait trouver explicitement dans les revendications indépendantes.

En conséquence, la revendication 1 n'est pas claire et ne satisfait pas aux conditions requises à l'Article 6 PCT, dans la mesure où l'objet pour lequel une protection est demandée n'est pas clairement défini. Telle qu'elle a été spécifiée, la définition fonctionnelle ci-dessus ne permet pas à l'homme du métier de déterminer quelles sont les caractéristiques techniques nécessaires à la réalisation de la fonction.

1b. La revendication de procédé 1 n'est pas claire en ce qu'elle ne contient pas **toutes les caractéristiques techniques essentielles** nécessaires à la définition de l'invention, conformément aux exigences de l'Article 6 PCT pris en combinaison avec la Règle 6.3(b) PCT.

- En effet la revendication 1 ne précise pas comment les premiers (TC0) et les autres moyens (TC1) sont réalisés. Cette caractéristique (c.-à-d. des **tables de constantes**) est cependant essentielle, compte tenu de la description pages 15-16. De plus, aucune autre solution n'est considérée, de sorte qu'une telle **généralisation n'est pas supportée par la description**.

  Cette caractéristique aurait pû être tirée de la revendication 10.

- Par ailleurs, la caractéristique de la revendication 2 est aussi **essentielle** et aurait dû être ajoutée à la revendication 1 parce que, sans cette caractéristique, les données dérivées du procédé de la revendication 1 ne seraient pas imprédictibles. Cette caractéristique essentielle est cependant contenue dans la revendication de dispositif 11. Le Demandeur est prié de supprimer cette discordance.

1c. La revendication **indépendante** de dispositif 11 **devrait contenir** explicitement, même si la référence aux revendications de procédé 1-10 est maintenue, **toutes** les caractéristiques techniques essentielles (c.-à-d. celles se référant aux autres moyens TC1) nécessaires à la définition de l'invention (Article 6 en combinaison avec la Règle 6.3(b) PCT). Ces caractéristiques pourraient avoir être tirées de la revendication de procédé 1.

1d. En outre, les revendications indépendantes 1, 11 et 12 ne précisent pas que le procédé de contre-mesure s'applique à l'algorithme de cryptographie à clé secrète **DES**. Cependant, il ressort clairement de la description que cette caractéristique est essentielle à la définition de l'invention parce que toute l'analyse du problème d'une attaque DPA à un algorithme à clé secrète et sa solution est fondée sur cette caractéristique particulière.

Cette **généralisation ne se fonde pas sur la description**, comme l'exige l'Article 6 PCT.

Eu égard à la description page 9, lignes 12-16 et page 21, lignes 12-15, il est jugé utile de préciser à ce stade de la procédure que, selon les Directives PCT C-III-6.5, "une revendication peut définir de façon générale une caractéristique par rapport à sa fonction, même lorsqu'un seul exemple de la caractéristique a été donné dans la description... ...En général, toutefois, si le contenu de la demande est tel qu'il conduit à penser qu'une fonction doit être assurée d'une façon déterminée, sans évoquer la possibilité de variantes, et si une revendication est formulée de telle façon qu'elle englobe d'autres moyens ou tous les moyens d'assurer cette fonction, **il y a lieu de faire objection**. En outre, une insuffisance peut résulter du fait que la description se borne à indiquer en termes vagues que d autres moyens peuvent être adoptés, **s'il n'y en ressort pas clairement que** ces autres moyens pourraient être utilisés et comment ils pourraient l'être".

1c. De plus, les termes "donnée d'entrée", "donnée de sortie", "données dérivées" dans les revendications 1 et 11 ne sont pas claires (Article 6 PCT) parce qu'il n'est pas possible de comprendre où celles-ci entrent, d'où sortent et d'où sont dérivées.

2. La formulation "les autres moyens (TC1, **TC2**)" utilisée dans la revendication dépendante 6 n'est pas claire (Article 6 PCT) parce qu'aucun autre moyen TC2 n'a été défini auparavant dans les revendications 1 ou 2.

NOUVELLES REVENDICATIONS

1. Procédé de contre-mesure contre des attaques par analyse différentielle de consommation en courant dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (K), la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers moyens (TC_0) de traitement numérique pour fournir une donnée de sortie (S) à partir d'une donnée d'entrée (E), ladite donnée de sortie et/ou des données dérivées de cette donnée de sortie étant manipulées par des instructions dudit algorithme, qui sont critiques au sens des dites attaques, caractérisé en ce que le procédé de contre-mesure prévoit l'utilisation d'autres moyens (TC_1) de traitement numérique, de façon alternative avec lesdits premiers moyens, lesdits autres moyens étant obtenus desdits premiers moyens par complémentation de la donnée d'entrée et/ou de la donnée de sortie, en sorte que la donnée de sortie et lesdites données dérivées soient imprédictibles.

2. Procédé de contre-mesure selon la revendication 1, caractérisé en ce que l'utilisation des différents moyens (TC_0, TC_1) est gérée par une loi statistique de probabilité un demi.

3. Procédé de contre-mesure selon la revendication 2, la mise en oeuvre de l'algorithme comprenant seize tours de calcul (T1, ...,T16), caractérisé en ce qu'il comprend l'exécution d'une première séquence (SEQA) et d'une deuxième séquence (SEQB) formées des trois premiers tours au moins (T1, T2, T3), l'ordre d'exécution des séquences étant fonction de la loi statistique de probabilité un demi, la première

séquence (SEQA) utilisant les premiers moyens (TC_0) dans chaque tour, la deuxième séquence (SEQB) utilisant les autres moyens (TC_1) dans le premier tour (T1) au moins.

4. Procédé de contre-mesure selon la revendication 3, caractérisé en ce que la première et la deuxième séquences sont formées chacune des trois premiers tours (T1, T2, T3).

5. Procédé de contre-mesure selon la revendication 3 ou 4, caractérisé en ce que les autres moyens consistent en des deuxièmes moyens (TC_1) tels que pour une même donnée d'entrée (E), ils fournissent en sortie le complément (/S) de la donnée de sortie (S) des premiers moyens (TC_0).

6. Procédé de contre-mesure selon la revendication 2, la mise en oeuvre de l'algorithme comprenant seize tours de calcul (T1, ...,T16), caractérisé en ce qu'il comprend l'exécution d'une première séquence (SEQA') et d'une deuxième séquence (SEQB') formées chacune des trois derniers tours (T14, T15, T16) au moins, l'ordre d'exécution des séquences étant fonction de la loi statistique de probabilité un demi, la première séquence (SEQA') utilisant les premiers moyens (TC_0) dans chaque tour, la deuxième séquence (SEQB') utilisant les autres moyens (TC_1, TC_2).

7. Procédé de contre-mesure selon la revendication 6, caractérisé en ce que la première et la deuxième séquences sont formées chacune des trois derniers tours, et en ce que les autres moyens utilisés dans la

deuxième séquence comprennent des deuxièmes moyens (TC_1) et des troisièmes moyens (TC_2).

8. Procédé de contre-mesure selon la revendication 6 ou 7, caractérisé en ce que les deuxièmes moyens (TC_1) sont tels que pour une même donnée d'entrée (E), ils fournissent en sortie le complément (/S) de la donnée de sortie (S) des premiers moyens (TC_0) et en ce que ces deuxièmes moyens sont utilisés dans la deuxième séquence (SEQB') pour le quatorzième tour (T14).

9. Procédé de contre-mesure selon la revendication 8, caractérisé en ce que les troisièmes moyens (TC_2) sont tels que pour le complément de la donnée d'entrée (E), ils fournissent en sortie le complément (/S) de la donnée de sortie (S) des premiers moyens (TC_0) et sont utilisés dans la deuxième séquence, pour le quinzième tour et le seizième tour (T15, T16).

10. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens sont des tables de constantes.

11. Composant électronique comprenant un microprocesseur, une mémoire programme et une mémoire de travail permettant la mise en oeuvre d'un algorithme cryptographique à clé secrète (K), des premiers moyens (TC_0) de traitement numérique étant prévus pour fournir une donnée de sortie (S) à partir d'une donnée d'entrée (E), ladite donnée de sortie et/ou des données dérivées de cette donnée de sortie étant manipulées par des instructions critiques dudit algorithme au sens d'attaques par analyse différentielle de consommation en courant, caractérisé en ce qu'il comprend des moyens

de mise en oeuvre d'un procédé de contre-mesure contre lesdites attaques selon l'une quelconque des revendications 1 à 10 précédentes, comprenant d'autres moyens de (TC_1) de traitement numérique fixés avec les premiers moyens en mémoire programme du dit composant, et des moyens de génération d'une valeur aléatoire (RND1) à 0 ou à 1 pour gérer l'utilisation des dits premiers moyens et autres moyens (TC_0, TC_1).

12. Carte à puce comprenant un composant électronique selon la revendication 11.

09/807607
Translation
2131

RECEIVED
AUG 0 6 2001
Technology Center 2100

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM 587	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/02172	International filing date (*day/month/year*) 13 September 1999 (13.09.99)	Priority date (*day/month/year*) 16 October 1998 (16.10.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/06		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 9 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 15 May 2000 (15.05.00)	Date of completion of this report 24 January 2001 (24.01.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR99/02172

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:
pages 1-22 . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☒ the claims:
pages _____ . as originally filed
pages _____ . as amended (together with any statement under Article 19
pages _____ . filed with the demand
pages 1-12 . filed with the letter of 16 October 2000 (16.10.2000)

☒ the drawings:
pages 1/8-8/8 . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☐ the sequence listing part of the description:
pages _____ . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:
☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 99/02172

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-12	YES
	Claims		NO
Inventive step (IS)	Claims	1-12	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following documents cited in the International Search Report:

D1: YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 November 1997, pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

D2: MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 July 1994, pages 85-90, XP000460342

D3: FR-A-2 672 402 (GEMPLUS CARD INT) 7 August 1992

1. The present application concerns a countermeasure method (Claim 1) in an electronic component using a secret key cryptographic algorithm (DES) for calculating an enciphered message on the basis of an input message.

It also concerns an electronic component (Claim 11) and a smart card (Claim 12) implementing the

countermeasure method.

These algorithms are vulnerable to attacks based on differential power consumption analysis (DPA). The characteristics of the algorithms are known and certain calculated data depend only on the plaintext input into the card and on the secret key contained in the card. Normally, for each specific data bit there is a corresponding sub-key formed by a specific group of key bits. The basic idea of the DPA attack is to use the variation in the power consumption pattern of an instruction according to whether it is manipulating a 0 or a 1, and the possibility of calculating a target bit (predictable bit) based on a known input or output message and a hypothesis concerning the corresponding sub-key.

The aim of the present invention is to implement a countermeasure method in an electronic component which causes a null DPA signal even if the hypothesis for the sub-key is correct. It allows target bits to be made unpredictable by making it equally probable that a target bit will have the value 1 or 0.

The solution of the invention consists of introducing into some cycles of the algorithm an alternative performance sequence whose results at the output of the last cycle are the same as the results of the original sequence and whose predictable data bits complement those in the original sequence.

2. None of the documents cited in the International

Search Report describes a countermeasure method in an electronic component against attacks based on differential power consumption analysis.

- D1 describes a method for developing strong S-boxes (substitution boxes) easily and efficiently by computer. The DES could be broken if weak S-boxes were used. The reverse boxes are equally strong. The method performs well against differential attack.

- D2 refers to a principal secret encipherment algorithm which changes dynamically under the control of the encipherment key. The method is resistant to attacks which calculate the key by using plaintext and ciphertext block pairs. It contains an example with a modified DES code.

- D3 concerns a method and device for generating unique pseudo-random numbers by using the DES algorithm applied in making smart cards.

3. Such a solution has thus not been described and cannot be derived from the documents cited, and an inventive step is recognised. Therefore Claims 1, 11 and 12 meet the requirements of PCT Article 33.

4. Claims 2 to 10 depend on Claim 1 and therefore also, as such, satisfy the requirements of PCT Article 33 regarding novelty and inventive step.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. In order to meet the requirements set out in PCT Rule 5.1(a)(ii), the applicant should have cited in the description documents D1 to D3 or other documents constituting the prior art such as described in the introduction to the description (pages 1 to 8 and 11 to 15), and should have indicated the corresponding prior art. He should also have identified those documents in accordance with PCT Rule 5.1 (a) (ii).

2. In order to meet the requirements set out in PCT Rule 5.1(a)(iii), the introductory part of the description should have been brought into line with the new claims put forward by the applicant.

3. The applicant could have taken the opportunity of making these amendments to correct typographical errors in the application:

- "constant" (page 16, line 2) should be plural.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. As regards the independent claims:

1a. The wording "it provides for the use of other means (TC1) . . . **so that** the output data and the derived data cannot be predicted" used in Claim 1 attempts to **define the invention by the result to be achieved**.

Such wording is not sufficient (see PCT Guidelines C-III-4.7 which specify that claims attempting to define the invention by the result sought are not permitted), as it does not contain all the essential features necessary to define the invention (Article 6, in combination with PCT Rule 6.3(b)). Indeed, it is rather the features which define **what these means are and how said means are arranged, connected and used** so that this result may be achieved that should be explicitly stated in the independent claims.

Consequently, Claim 1 is not clear and does not satisfy the requirements of PCT Article 6, to the extent that the subject matter for which protection is sought is not clearly defined. The above functional definition as specified does not enable a person skilled in the art to determine the technical features required for carrying out said function.

1b. Method Claim 1 is not clear in that it does not contain **all the essential technical features** necessary to define the invention in accordance with the requirements of PCT Article 6 taken in

VIII. Certain observations on the international application

combination with PCT Rule 6.3(b).

- Indeed, Claim 1 does not specify how the first (TC0) and other means (TC1) are achieved. This feature (i.e. **tables of constants**) is, however, essential, taking into account the description, pages 15 and 16. Moreover, no other solution is considered, so that such a **generalisation is not supported by the description**.

  This feature could have been drawn from Claim 10.

- Besides, the feature of Claim 2 is also **essential** and should have been added to Claim 1 because, without this feature, the data derived from the method of Claim 1 would not be unpredictable. This essential feature is, however, contained in the device Claim 11. The applicant is requested to remove this discrepancy.

1c. Even if the reference to the method Claims 1 to 10 is kept, the **independent** device Claim 11 **should explicitly** contain **all** the essential technical features (i.e. those referring to the other means TC1) necessary to define the invention (Article 6 in combination with PCT Rule 6.3(b)).
These features could have been drawn from method Claim 1.

1d. Moreover, independent Claims 1, 11 and 12 do not specify that the countermeasure method applies to the **DES** secret key cryptographic algorithm.
However, it emerges clearly from the description

VIII. Certain observations on the international application

that this feature is essential to define the invention because the whole analysis of the problem of a DPA attack on a secret key algorithm and its solution is based on this specific feature.

This **generalisation is not based on the description** as required by PCT Article 6.

Taking into account the description, page 9, lines 12 to 16 and page 21, lines 12 to 15, it is considered useful to specify at this stage in the proceedings that, according to PCT Guidelines C-III-6.5, "a claim may broadly define a feature in terms of its function, even where only one example of the feature has been given in the description . . . . . In general, however, if the entire contents of the application are such as to convey the impression that a function is to be carried out in a particular way, with no intimation that alternative means are envisaged, and a claim is formulated in such away as to embrace other means, or all means, of performing the function, then **objection** arises. Furthermore, it may not be sufficient if the description merely states in vague terms that other means may be adopted, **if it is not reasonably clear** what they might be or how they might be used".

1c. Moreover, the terms "input data", "output data", "derived data" in Claims 1 and 11 are not clear (PCT Article 6), because one cannot understand where the data goes in, from where they exit and from what they are derived.

VIII. Certain observations on the international application

2. The wording "the other means (TC1, **TC2**)" used in dependent Claim 6 is not clear (PCT Article 6), because no other means TC2 has been defined earlier in Claims 1 or 2.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/06	A1	(11) Numéro de publication internationale: WO 00/24155
		(43) Date de publication internationale: 27 avril 2000 (27.04.00)

(21) Numéro de la demande internationale: PCT/FR99/02172

(22) Date de dépôt international: 13 septembre 1999 (13.09.99)

(30) Données relatives à la priorité:
98/12989 16 octobre 1998 (16.10.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: CLAVIER, Christophe [FR/FR]; 5 rue de la République, F-13420 Gémenos (FR). BENOIT, Olivier [FR/FR]; La Treille d'Azur, Bâtiment D. avenue 19 Mars 1962, F-13400 Aubagne (FR).

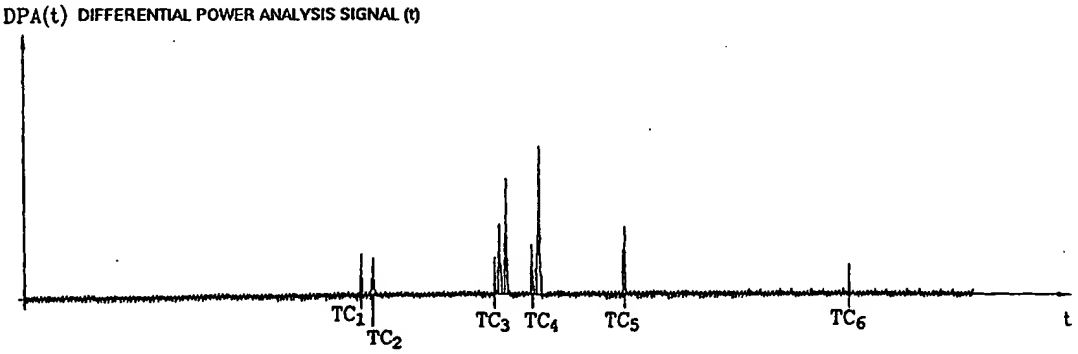
(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos Cedex (FR).

(81) Etats désignés: AU, CA, CN, IN, JP, MX, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM

(54) Titre: PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE



(57) Abstract

The invention concerns a countermeasure method in an electronic component using a secret key K cryptographic algorithm, wherein the algorithm implementation comprises the use of first means TC_0 for supplying output data from input data, the output information and/or derived data being manipulated by critical instructions. Said countermeasure method provides for the use of other means TC_1 and/or TC_2, such that the output information and the derived data are unpredictable.

(57) Abrégé

Dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète K, la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers moyens TC_0 pour fournir une donnée de sortie S à partir d'une donnée d'entrée E, la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques, un procédé de contre-mesure prévoit l'utilisation d'autres moyens TC_1 et/ou TC_2, en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROCÉDÉ DE CONTRE-MESURE DANS UN COMPOSANT ÉLECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLÉ SECRETE

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé secrète. Ils sont utilisés dans des applications où l'accès à des services ou à des données est sévèrement contrôlé. Ils ont une architecture formée autour d'un microprocesseur et de mémoires, dont une mémoire programme qui contient la clé secrète.

Ces composants sont notamment utilisés dans les cartes à puce, pour certaines applications de celles-ci. Ce sont par exemple des applications d'accès à certaines banques de données, des applications bancaires, des applications de télépéage, par exemple pour la télévision, la distribution d'essence ou encore le passage de péages d'autoroutes.

Ces composants ou ces cartes mettent donc en oeuvre un algorithme de cryptographie à clé secrète, dont le plus connu est l'algorithme DES (pour *Data Encryption Standard* dans la littérature anglo-saxonne). D'autres algorithmes à clé secrète existent, comme l'algorithme RC5 ou encore l'algorithme COMP128. Cette liste n'est bien sûr pas exhaustive.

De manière générale et succincte, ces algorithmes ont pour fonction de calculer un message chiffré à partir d'un message appliqué en entrée (à la carte) par un système hôte (serveur, distributeur bancaire...) et de la clé secrète contenue dans la carte, et de fournir en retour au système hôte ce message chiffré, ce qui permet par exemple au système hôte d'authentifier le composant ou la carte, d'échanger des données...

Or il est apparu que ces composants ou ces cartes sont vulnérables à des attaques consistant en une analyse différentielle de consommation en courant et qui permettent à des tiers mal intentionnés de trouver la clé secrète. Ces attaques sont appelées attaques DPA, acronyme anglo-saxon pour *Differential Power Analysis*.

Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

Notamment, une instruction du microprocesseur manipulant un bit de donnée génère deux profils de courant différents selon que ce bit vaut "1" ou "0". Typiquement, si l'instruction manipule un "0", on a à cet instant d'exécution une première amplitude du courant consommé et si l'instruction manipule un "1", on a une deuxième amplitude du courant consommé, différente de la première.

Les caractéristiques des algorithmes de cryptographie sont connues : calculs effectués, paramètres utilisés. La seule inconnue est la clé secrète contenue en mémoire programme. Celle-ci ne peut être déduite de la seule connaissance du message appliqué en entrée et du message chiffré fourni en retour.

Cependant, dans un algorithme de cryptographie, certaines données calculées dépendent seulement du message appliqué en clair en entrée de la carte et de la clé secrète contenue dans la carte. D'autres données calculées dans l'algorithme peuvent aussi être recalculées seulement à partir du message chiffré (généralement fourni en clair en sortie de la carte vers le système hôte) et de la clé secrète contenue dans la carte. Plus précisément, chaque bit de ces données particulières peut être déterminé à partir du

message d'entrée ou de sortie, et d'un nombre limité de bits particuliers de la clé.

Ainsi, à chaque bit d'une donnée particulière, correspond une sous-clé formée par un groupe particulier de bits de la clé.

Les bits de ces données particulières qui peuvent être prédites sont appelés dans la suite, bits cibles.

L'idée de base de l'attaque DPA est ainsi d'utiliser la différence du profil de consommation en courant d'une instruction selon qu'elle manipule un "1" ou un "0" et la possibilité de calculer un bit cible par les instructions de l'algorithme à partir d'un message connu d'entrée ou de sortie et d'une hypothèse sur la sous-clé correspondante.

Le principe de l'attaque DPA est donc de tester une hypothèse de sous-clé donnée, en appliquant sur un grand nombre de courbes de mesure en courant, chacune relative à un message d'entrée connu de l'attaquant, une fonction booléenne de sélection, fonction de l'hypothèse de sous-clé, et définie pour chaque courbe par la valeur prédite pour un bit cible.

En faisant une hypothèse sur la sous-clé concernée, on est en effet capable de prédire la valeur "0" ou "1" que va prendre ce bit cible pour un message d'entrée ou de sortie donné.

On peut alors appliquer comme fonction booléenne de sélection, la valeur prédite "0" ou "1" par le bit cible pour l'hypothèse de sous-clé considérée, pour trier ces courbes en deux paquets : un premier paquet regroupe les courbes qui ont vu la manipulation du bit cible à "0" et un deuxième paquet regroupe les courbes qui ont vu la manipulation du bit cible à "1" selon l'hypothèse de sous-clé. En faisant la moyenne de consommation en courant dans chaque paquet, on obtient une courbe de consommation moyenne M0 (t) pour le

premier paquet et une courbe de consommation moyenne M1(t) pour le deuxième paquet.

Si l'hypothèse de sous-clé est juste, le premier paquet regroupe réellement toutes les courbes parmi les N courbes qui ont vu la manipulation du bit cible à "0" et le deuxième paquet regroupe réellement toutes les courbes parmi les N courbes qui ont vu la manipulation du bit cible à "1". La courbe moyenne de consommation M0(t) du premier paquet aura alors une consommation moyenne partout sauf aux moments de l'exécution des instructions critiques, avec un profil de consommation en courant caractéristique de la manipulation du bit cible à "0" ($profil_0$). En d'autres termes, pour toutes ces courbes tous les bits manipulés ont eu autant de chances de valoir "0" que de valoir "1", sauf le bit cible qui a toujours eu la valeur "0". Ce qui peut s'écrire :

$M0(t)=[(profil_0+profil_1)/2]_{t\neq tci} + [profil_0]_{tci}$ soit

$M0(t)=[Vm_t]_{t\neq tci} + [profil_0]_{tci}$

où tci représente les instants critiques, auxquels une instruction critique a été exécutée.

De même, la courbe moyenne de consommation M1(t) du deuxième paquet correspond à une consommation moyenne partout sauf aux moments de l'exécution des instructions critiques, avec un profil de consommation en courant caractéristique de la manipulation du bit cible à "1" ($profil_1$). On peut écrire :

$M1(t)=[(profil_0+profil_1)/2]_{t\neq tci} + [profil_1]_{tci}$ soit

$M1(t)=[Vm_t]_{t\neq tci} + [profil_1]_{tci}$

On a vu que les deux profils $profil_0$ et $profil_1$ ne sont pas égaux. La différence des courbes M0(t) et M1(t) donne alors un signal DPA(t) dont l'amplitude est égale à $profil_0-profil_1$ aux instants critiques tci d'exécution des instructions critiques manipulant ce bit, c'est à dire, dans l'exemple représenté sur la figure 1, aux endroits tc0 à tc6, et dont l'amplitude

est à peu près égale à zéro en dehors des instants critiques.

Si l'hypothèse de sous-clé est fausse, le tri ne correspond pas à la réalité. Statistiquement, il y a alors dans chaque paquet, autant de courbes ayant vu réellement la manipulation du bit cible à "0" que de courbes ayant vu la manipulation du bit cible à "1". La courbe moyenne résultante M0(t) se situe alors autour d'une valeur moyenne donnée par $(profil_0+profil_1)/2=Vm$, car pour chacune des courbes, tous les bits manipulés, y compris le bit cible ont autant de chances de valoir "0" que de valoir "1".

Le même raisonnement sur le deuxième paquet conduit à une courbe moyenne de consommation en courant M1(t) dont l'amplitude se situe autour d'une valeur moyenne donnée par $(profil_0+profil_1)/2=Vm$.

Le signal DPA(t) fourni par la différence M0(t)-M1(t) est dans ce cas sensiblement égal à zéro. Le signal DPA(t) dans le cas d'une hypothèse de sous-clé fausse est représenté sur la figure 2.

Ainsi l'attaque DPA exploite la différence du profil de consommation en courant pendant l'exécution d'une instruction suivant la valeur du bit manipulé, pour effectuer un tri de courbes de consommation en courant selon une fonction de sélection booléenne pour une hypothèse de sous-clé donnée. En effectuant une analyse différentielle de la consommation moyenne en courant entre les deux paquets de courbes obtenus, on obtient un signal d'information DPA(t).

Le déroulement d'une attaque DPA consiste alors globalement:

a- à tirer N messages aléatoires (par exemple N égal 1000);

b- à faire exécuter l'algorithme par la carte pour chacun des N messages aléatoires, en relevant la courbe

de consommation en courant à chaque fois (mesurée sur la borne d'alimentation du composant);

c- à faire une hypothèse sur une sous-clé;

d- à prédire, pour chacun des messages aléatoires, la valeur prise par un des bits cibles dont la valeur ne dépend que des bits du message (d'entrée ou de sortie) et de la sous-clé prise en hypothèse, pour obtenir la fonction de sélection booléenne;

e- à trier les courbes selon cette fonction de sélection booléenne (c'est à dire selon la valeur "0" ou "1" prédite pour ce bit cible pour chaque courbe sous l'hypothèse de sous-clé);

f- à calculer dans chaque paquet la courbe résultante de consommation moyenne en courant;

g- à effectuer la différence de ces courbes moyennes, pour obtenir le signal DPA(t).

Si l'hypothèse sur la sous-clé est juste, la fonction de sélection booléenne est juste et les courbes du premier paquet correspondent réellement aux courbes pour lesquelles le message appliqué en entrée ou en sortie a donné un bit cible à "0" dans la carte et les courbes du deuxième paquet correspondent réellement aux courbes pour lesquelles le message appliqué en entrée ou en sortie a donné un bit cible à "1" dans la carte.

On est dans le cas de la figure 1 : le signal DPA(t) n'est donc pas nul aux instants tc0 à tc6 correspondant à l'exécution des instructions critiques (celles qui manipulent le bit cible).

On notera que l'attaquant n'a pas besoin de connaître avec précision les instants critiques. Il suffit qu'il y ait au moins un instant critique dans la période d'acquisition.

Si l'hypothèse de sous-clé n'est pas juste, le tri ne correspond pas à la réalité et on a alors dans chaque paquet autant de courbes correspondant en

réalité à un bit cible à "0" que de courbes correspondant à un bit cible à "1". Le signal DPA(t) est sensiblement nul partout (cas représenté à la figure 2). Il faut retourner à l'étape c- et faire une nouvelle hypothèse sur la sous-clé.

Si l'hypothèse s'avère juste, on peut passer à l'évaluation d'autres sous-clés, jusqu'à avoir reconstitué la clé au maximum. Par exemple, avec un algorithme DES, on utilise une clé de 64 bits, dont seulement 56 bits utiles. Avec une attaque DPA, on est capable de reconstituer au moins 48 bits des 56 bits utiles.

La présente invention a pour but de mettre en oeuvre dans un composant électronique, un procédé de contre-mesure qui entraîne un signal DPA(t) nul, même dans le cas où l'hypothèse de sous-clé est juste.

De cette façon, rien ne permet de distinguer le cas de l'hypothèse de sous-clé juste des cas d'hypothèses de sous-clé fausses. Par cette contre-mesure, le composant électronique est paré contre les attaques DPA.

Selon l'invention, le procédé de contre-mesure permet de rendre imprédictibles les bits cibles, c'est à dire les données manipulées par des instructions critiques.

En effet, du fait de la contre-mesure, pour chaque message appliqué en entrée, un bit cible manipulé par une instruction critique prend la valeur 0 ou 1 avec une égale probabilité. Dans chaque paquet de courbes que fera l'attaquant sous une hypothèse de sous-clé donnée, au moyen de la fonction de sélection booléenne qu'il aura calculée, on aura autant de courbes ayant réellement manipulé un bit cible "0" que de courbes ayant réellement manipulé un bit cible à "1". Le signal DPA(t) sera toujours nul, que l'hypothèse de sous-clé soit juste ou non.

Telle que caractérisée, l'invention concerne donc un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète, la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers moyens pour fournir une donnée de sortie à partir d'une donnée d'entrée, la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques. Selon l'invention, le procédé de contre-mesure prévoit l'utilisation d'autres moyens, en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

Selon l'invention, l'utilisation des différents moyens est gérée selon une loi statistique de probabilité un demi.

D'autres caractéristiques et avantages de l'invention sont détaillés dans la description suivante faite à titre indicatif et nullement limitatif et en référence aux dessins annexés, dans lesquels :

- les figures 1 et 2 déjà décrites représentent le signal DPA(t) que l'on peut obtenir en fonction d'une hypothèse sur une sous-clé de la clé secrète K, selon une attaque DPA;
- les figures 3 et 4 sont des organigrammes d'exécution des premiers tours et derniers tours de l'algorithme DES;
- la figure 5 est un schéma-bloc de l'opération SBOX utilisée dans l'algorithme DES;
- la figure 6 montre un exemple de table de constante élémentaire à une entrée et une sortie utilisée dans l'opération SBOX;
- les figures 7 et 8 montrent un exemple d'organigramme d'exécution des premiers et derniers tours de l'algorithme DES, selon un mode de réalisation du procédé de contre-mesure selon l'invention;

- les figures 9 et 10 montrent respectivement une deuxième et une troisième tables de constantes élémentaires selon l'invention;

- la figure 11 représente un organigramme général d'exécution du DES selon un mode de réalisation du procédé de contre-mesure selon l'invention; et

- la figure 12 représente un schéma-bloc simplifié d'une carte à puce comportant un composant électronique dans lequel le procédé de contre-mesure selon l'invention est mis en oeuvre.

La présente invention va être expliquée dans un exemple d'application à l'algorithme cryptographique DES. L'invention n'est pas limitée à ce seul exemple. Elle s'applique aux algorithmes cryptographiques à clé secrète en général.

L'algorithme cryptographique DES (dans la suite on parlera plus simplement du DES ou de l'algorithme DES) comporte 16 tours de calcul, notés T1 à T16, comme représenté sur les figures 3 et 4.

Le DES débute par une permutation initiale IP sur le message d'entrée M (figure 3). Le message d'entrée M est un mot f de 64 bits. Après permutation, on obtient un mot e de 64 bits, que l'on coupe en deux pour former les paramètres d'entrée L0 et R0 du premier tour (T1). L0 est un mot d de 32 bits contenant les 32 bits de poids forts du mot e. R0 est un mot h de 32 bits contenant les 32 bits de poids faibles du mot e.

La clé secrète K, qui est un mot q de 64 bits subit elle-même une permutation et une compression pour fournir un mot r de 56 bits.

Le premier tour comprend une opération EXP PERM sur le paramètre R0, consistant en une expansion et une permutation, pour fournir en sortie un mot l de 48 bits.

Ce mot l est combiné à un paramètre K1, dans une opération de type OU EXCLUSIF notée XOR, pour fournir un mot b de 48 bits. Le paramètre K1 qui est un mot m de 48 bits est obtenu du mot r par un décalage d'une position (opération notée SHIFT sur les figures 3 et 4) suivi d'une permutation et d'une compression (opération notée COMP PERM).

Le mot b est appliqué à une opération notée SBOX, en sortie de laquelle on obtient un mot a de 32 bits. Cette opération particulière sera expliquée plus en détail en relation avec les figures 5 et 6.

Le mot a subit une permutation P PERM, donnant en sortie le mot c de 32 bits.

Ce mot c est combiné au paramètre d'entrée L0 du premier tour T1, dans une opération logique de type OU EXCLUSIF, notée XOR, qui fournit en sortie le mot g de 32 bits.

Le mot h (=R0) du premier tour fournit le paramètre d'entrée L1 du tour suivant (T2) et le mot g du premier tour fournit le paramètre d'entrée R1 du tour suivant. Le mot p du premier tour fournit l'entrée r du tour suivant.

Les autres tours T2 à T16 se déroulent de façon similaire, excepté en ce qui concerne l'opération de décalage SHIFT qui se fait sur une ou deux positions selon les tours considérés.

Chaque tour Ti reçoit ainsi en entrée les paramètres Li-1, Ri-1 et r et fournit en sortie les paramètres Li, Ri et r pour le tour suivant Ti+1.

En fin d'algorithme DES (figure 4), le message chiffré est calculé à partir des paramètres L16 et R16 fournis par le dernier tour T16.

Ce calcul du message chiffré C comprend en pratique les opérations suivantes :

- formation d'un mot e' de 64 bits en inversant la position des mots L16 et R16, puis en les concaténant;

- application de la permutation IP^{-1} inverse de celle de début de DES, pour obtenir le mot f' de 64 bits formant le message chiffré C.

L'opération SBOX est détaillée sur les figures 5 et 6. Elle comprend une table de constantes TC_0 pour fournir une donnée de sortie a en fonction d'une donnée d'entrée b.

En pratique, cette table de constantes TC_0 se présente sous la forme de huit tables de constantes élémentaires TC_01 à TC_08, chacune recevant en entrée seulement 6 bits du mot b, pour fournir en sortie seulement 4 bits du mot a.

Ainsi, la table de constante élémentaire TC_01 représentée sur la figure 6 reçoit comme donnée d'entrée, les bits b1 à b6 du mot b et fournit comme donnée de sortie les bits a1 à a4 du mot a.

En pratique ces huit tables de constantes élémentaires sont mémorisées en mémoire programme du composant électronique.

Dans l'opération SBOX du premier tour T1, un bit particulier de la donnée a de sortie de la table de constante TC_0 dépend de seulement 6 bits de la donnée b appliquée en entrée, c'est à dire de seulement 6 bits de la clé secrète K et du message d'entrée (M).

Dans l'opération SBOX du dernier tour T16, un bit particulier de la donnée a de sortie de la table de constante TC_0 peut être recalculé à partir de seulement 6 bits de la clé secrète K et du message chiffré (C).

Or si on reprend le principe de l'attaque DPA, si on choisit comme bit cible un bit de la donnée de sortie a, il suffit de faire une hypothèse sur 6 bits de la clé K, pour prédire la valeur d'un bit cible pour un message d'entrée (M) ou de sortie (C) donné. En d'autres termes, pour le DES, il suffit de faire une hypothèse sur une sous-clé de 6 bits.

Dans une attaque DPA sur un tel algorithme pour un bit cible donné, on a donc à discriminer une hypothèse de sous-clé juste parmi 64 possibles.

Ainsi, en prenant seulement huit bits du mot a comme bits cibles, (un bit de sortie par table de constantes élémentaire $TC_0 1$ à $TC_0 8$), on peut découvrir jusqu'à 6x8=48 bits de la clé secrète, en faisant des attaques DPA sur chacun de ces bits cibles.

Dans le DES, on trouve donc des instructions critiques au sens des attaques DPA au début de l'algorithme et à la fin.

Au début de l'algorithme DES, les données qui peuvent être prédites à partir d'un message d'entrée M et d'une hypothèse de sous-clé, sont les données a et g calculées dans le premier tour (T1).

La donnée a du premier tour T1 (figure 3) est la donnée de sortie de l'opération SBOX du tour considéré. La donnée g est calculée à partir de la donnée a, par permutation (P PERM) et opération OU EXCLUSIF avec le paramètre d'entrée L0.

En fait, la donnée c du premier tour, est une donnée dérivée de la donnée a du premier tour. La donnée dérivée c correspond à une simple permutation de bits de la donnée a.

La donnée l du deuxième tour est une donnée dérivée de la donnée g du premier tour, car elle correspond à une permutation des bits du mot g, certains bits du mot g étant en outre dupliqués.

Connaissant a et g, on peut aussi connaître ces données dérivées.

Les instructions critiques du début de l'algorithme sont les instructions critiques qui manipulent soit la donnée que l'on peut prédire, comme la donnée a du premier tour, soit une donnée dérivée.

Les instructions critiques manipulant la donnée a du premier tour T1 ou la donnée dérivée c sont ainsi

les instructions de fin de l'opération SBOX, de l'opération P PERM et de début de l'opération XOR du premier tour T1.

Les instructions critiques manipulant la donnée g ou des données dérivées sont toutes les instructions de fin d'opération XOR de fin du premier tour T1 jusqu'aux instructions de début d'opération SBOX du deuxième tour T2, et les instructions de début d'opération XOR de fin du troisième tour T3 (L2 = h(T2) = g(T1)).

En fin d'algorithme DES, les données qui peuvent être prédites à partir d'un message chiffré C et d'une hypothèse de sous-clé, sont la donnée a du seizième tour T16 et la donnée L15 égale au mot h du quatorzième tour T14.

Les instructions critiques manipulant la donnée a du seizième tour ou des données dérivées sont les instructions du seizième tour de fin d'opération SBOX, de l'opération de permutation P PERM et de début d'opération XOR.

Pour la donnée L15, les instructions critiques manipulant cette donnée ou des données dérivées sont toutes les instructions depuis les instructions de fin d'opération XOR du quatorzième tour T14, jusqu'aux instructions de début d'opération SBOX du quinzième tour T15, et les instructions de début d'opération XOR de fin du seizième tour T16.

Le procédé de contre-mesure selon l'invention appliqué à cet algorithme DES consiste à avoir, pour chaque instruction critique, autant de chances que l'instruction critique manipule une donnée que son complément. Ainsi, quel que soit le bit cible sur lequel l'attaque DPA peut être faite, on a autant de chances que les instructions critiques qui manipulent ce bit, manipulent un "1" ou un "0".

En pratique, ceci doit être vrai pour chacun des bits cibles potentiels : en d'autres termes,

l'attaquant ayant le choix entre plusieurs attaques possibles, c'est à dire entre plusieurs fonctions de sélection booléenne possibles pour effectuer son tri de courbes, pour une hypothèse de sous-clé donnée, la mise en oeuvre du procédé de contre-mesure selon l'invention doit s'attacher à ce que les données manipulées par chacune des instructions critiques, prennent aléatoirement, une fois sur deux, une valeur ou son complément. En ce qui concerne l'application du procédé de contre-mesure selon l'invention à l'algorithme DES, il faut donc appliquer la contre-mesure aux instructions critiques de début de DES et aux instructions critiques de fin de DES, pour être totalement protégé.

Dans le DES, toutes les données manipulées par des instructions critiques sont une donnée de sortie ou des données dérivées d'une donnée de sortie d'une opération SBOX.

En effet, en début de DES, les données qui peuvent être prédites sont les données a et g du premier tour T1. La donnée a est la donnée de sortie de l'opération SBOX du premier tour. La donnée g est calculée à partir de la donnée a, puisque g = P PERM(a) XOR L0. g est donc une donnée dérivée de la donnée de sortie a de l'opération SBOX du premier tour. Ainsi, toutes les données manipulées par les instructions critiques de début de DES découlent directement ou indirectement de la donnée de sortie a de l'opération SBOX du premier tour.

En ce qui concerne la fin de DES, les données qui peuvent être prédites sont la donnée a du seizième tour T16 et la donnée g du quatorzième tour T14, g étant égale à L15.

La donnée a est la donnée de sortie de l'opération SBOX du seizième tour T16.

Quant à la donnée L15, elle se calcule, dans l'exécution normale de l'algorithme DES, à partir de la donnée de sortie a de l'opération SBOX du quatorzième tour T14 : L15 = P PERM(a) XOR L14.

Si on rend imprédictibles les données de sortie a de ces opérations SBOX particulières, on rend aussi imprédictibles toutes les données dérivées : on rend donc imprédictibles toutes les données manipulées par les instructions critiques de l'algorithme DES.

L'opération SBOX correspond donc à des premiers moyens , qui consistent en une table de constantes TC_0, et qui sont utilisés dans chaque tour pour fournir une donnée de sortie E à partir d'une donnée d'entrée S.

Un mode de réalisation du procédé de contre-mesure appliqué à l'algorithme DES peut consister à utiliser au moins une autre table de constantes comme autres moyens pour rendre imprédictible la donnée de sortie a, en sorte que cette donnée de sortie et/ou des données dérivées manipulées par les instructions critiques soient toutes imprédictibles.

Dans l'exécution de l'algorithme, l'utilisation des diiférents moyens, c'est à dire, dans l'exemple, des différentes tables de constantes est gérée selon une loi statistique de probabilité un demi.

L'autre table de constantes ou les autres tables de constantes sont telles qu'à l'une et/ou l'autre des données d'entrée d et de sortie de la première table de constantes TC_0, elles font correspondre la donnée complémentée.

Les figures 7 et 8 représentent ainsi un mode d'application du procédé de contre-mesure de l'invention appliqué à l'algorithme DES.

La figure 7 représente le début de l'algorithme. Les opérations et données non modifiées par le procédé de contre-mesure selon l'invention portent les mêmes références que dans la figure 3 déjà décrite.

En début d'algorithme DES, on prévoit une deuxième table de constante TC_1 dans l'opération SBOX du premier tour T1. Toutes les données affectées par cette deuxième table de constantes TC_1 sont affectées d'un signe ' ou d'un signe ¯ sur ces figures. On voit que les instructions critiques de début de DES manipulent toutes des données affectées par le procédé de contre-mesure.

On remarquera que la première table de constantes étant en fait formée de huit premières tables de constantes, la deuxième table de constantes est également formée de huit deuxièmes tables de constantes.

Dans l'exemple de réalisation représenté, la première table de constantes TC_0 et la deuxième table de constantes TC_1 sont telles que pour une même donnée d'entrée E, la deuxième fournit en sortie le complément /S de la donnée de sortie S fournie par la première.

La figure 9 montre une telle deuxième table élémentaire $TC_1 1$ fournissant une sortie complémentée par rapport à la première table élémentaire $TC_0 1$ montrée sur la figure 6.

Avec une telle deuxième table de constantes TC_1, on obtient, en sortie de l'opération SBOX du premier tour T1, le complément /a de la donnée a obtenue avec la première table de constante TC_0. De même, on obtient dans le premier tour T1 la donnée complémentée /g et dans le deuxième tour T2, les données complémentées /h, /L2, /l et /b.

En utilisant la première table ou la deuxième table pour fournir la donnée de sortie selon une loi statistique de probabilité un demi, tous les bits de cible potentiels de début de DES manipulés par les instructions critiques ont autant de chances de prendre la valeur "1" que de prendre la valeur "0".

En fin d'algorithme DES, le mode de réalisation du procédé de contre-meseure selon l'invention nécessite l'utilisation de plusieurs tables de constantes différentes de la première, car il faut considérer à la fois la donnée de sortie a calculée au quatorzième tour T14, et la donnée de sortie a calculée au seizième tour T16 pour rendre imprédictibles toutes les données manipulées par les instructions critiques de cette fin de DES.

Un exemple de réalisation du procédé de contre-mesure appliqué à cette fin d'algorithme DES est représenté sur la figure 8.

Il prévoit l'utilisation de deux tables de constantes TC_1 et TC_2.

Dans l'opération SBOX du quatorzième tour T14, on utilise la deuxième table de constantes TC_1 déjà utilisée pour le début du DES.

Et on utilise une troisième table de constantes TC_2, dans les opérations SBOX des quinzième et seizième tours.

Cette troisième table de constantes TC_2 est telle qu'elle fournit le complément /S de la donnée de sortie S au complément /E de la donnée d'entrée E de la première table de constantes TC_0. Un exemple d'une troisième table de constantes élémentaire TC_21 correspondante, à partir de la première table de constantes élémentaire TC_0 est montré sur la figure 10.

En utilisant de telles tables de constantes, il apparaît sur la figure 8 que toutes les instructions critiques manipulent des données complémentées.

L'invention ne se limite pas à ces seuls exemples de tables de constantes TC_1 et TC_2. D'autres possibilités existent. Par exemple, pour le procédé de contre-mesure appliqué à la fin de DES, il est aussi possible de combiner l'utilisation de la table de constantes TC_1 avec une autre table de constantes

définie par rapport à la première table de constantes TC_0 comme fournissant la donnée de sortie S au complément /E de la donnée d'entrée.

D'une manière générale, la fin de DES nécessite l'utilisation de différentes tables de constantes, en fonction des tours considérés, pour que toutes les données manipulées par les instructions critiques de cette fin de DES soient imprédictibles.

Le mode de réalisation décrit en relation avec les figures 7 et 8 a cependant un inconvénient : le procédé de contre-mesure appliqué en entrée de DES produit des résultats intermédiaires calculés L3' et R3' qui ne sont pas justes. Tous les résultats intermédiaires suivants ne sont donc pas justes non plus.

De même, en fin de DES, le procédé de contre-mesure appliqué en entrée de DES produit des résultats intermédiaires calculés L16' et R16' qui ne sont pas justes.

Dans tous les cas, le message chiffré est faux.

Dans ce mode de réalisation de l'invention, il faut donc prévoir de pouvoir reprendre à chaque fois la suite de l'algorithme avec les bons résultats intermédiaires, une fois les instructions critiques passées.

En pratique, comme on a vu que les instructions critiques de début de DES se trouvent dans les trois premiers tours, on va dédoubler ces trois premiers tours. En d'autres termes, on prévoit d'exécuter deux séquences comprenant chacune les trois premiers tours T1, T2, T3 au moins. Une première séquence SEQA utilise la première table de constantes TC_0 dans chaque tour. L'autre séquence SEQB utilise la deuxième table de constantes TC_1 au moins dans le premier tour T1. Dans l'exemple représenté, on utilise la première table de constantes dans les deux tours suivants T2 et T3.

On a vu que dans le procédé de contre-mesure selon l'invention, l'utilisation des différents moyens, c'est à dire, dans l'exemple, l'utilisation des différentes tables de constantes, est gérée selon une loi statistique de probabilité un demi. Cette loi statistique de probabilité un demi est alors plus particulièrement appliquée à l'ordre d'utilisation de ces différents moyens, c'est à dire, dans l'exemple, à l'ordre d'éxécution des deux séquences SEQA et SEQB.

De même, pour avoir les bons paramètres L16 et R16 en fin de DES pour élaborer le message chiffré C, on dédouble également les trois tours T14, T15 et T16 (figure 7) qui contiennent les instructions critiques de fin de DES. On va donc exécuter deux séquences qui comprennent au moins les trois derniers tours T14, T15, T16. Une première séquence SEQA' utilise dans chaque tour la première table de constantes TC_0. L'autre séquence SEQB' utilise les autres tables de constantes TC_1 et TC_2. Comme précédemment, la loi statistique de probabilité un demi est alors appliquée à l'ordre d'exécution de ces deux séquences SEQA' et SEQB'.

Les instructions critiques sont alors exécutées deux fois, une dans chaque séquence. Mais au moment de l'exécution de n'importe laquelle des instructions critiques de l'une ou l'autre des séquences, la probabilité de manipuler une donnée sera égale à la probabilité de manipuler son complément.

Le programme de calcul du DES mis en oeuvre dans le composant électronique doit donc être modifié pour inclure le procédé de contre-mesure selon l'invention. Un exemple d'organigramme d'exécution conforme à l'invention et mettant en oeuvre le procédé de contre-mesure en début et en fin de DES selon le mode de réalisation décrit en relation avec les figures 7 et 8 est représenté sur la figure 11. Dans cet exemple, les séquences SEQA et SEQB comprennent les trois premiers

tours et les séquences SEQA' et SEQB' comprennent les trois derniers tours.

Le programme de calcul consiste alors principalement, au début du calcul, à sauvegarder les paramètres d'entrée notés DATAIN et KEY, qui correspondent en pratique aux paramètres L0, R0 et r, dans une zone mémoire temporaire notée CONTEXT0.

Selon ce programme de calcul, on positionne ensuite un premier compteur de boucle FR à 0, et on tire aléatoirement une valeur RND1 égale à 0 ou à 1.

Si RND1 vaut 1, dans l'exemple, on effectue d'abord la séquence SEQB de T1, T2, T3, dans laquelle on utilise la deuxième table de constantes TC_1 au tour T1 et la première table TC_0 pour les tours T2 et T3. On sauvegarde les paramètres de sortie L3', R3' (qui ont des valeurs fausses) dans une zone mémoire temporaire notée CONTEXT2.

Si FR n'est pas égal à 1, on le met à 1, on restaure les paramètres d'entrée du CONTEXT0 et on complémente la valeur de RND1. Dans l'exemple, on obtient RND1=0. On va alors exécuter l'autre séquence SEQA de T1, T2, T3 dans laquelle on utilise la première table de constante dans les trois tours T1, T2 et T3. On sauvegarde les paramètres de sortie (valeurs justes) dans une zone mémoire temporaire notée CONTEXT1.

Si FR est à 1, c'est que l'on a effectué les deux séquences. On restaure alors CONTEXT1 pour fournir les résultats intermédiaires L3, R3 ayant les valeurs justes, au tour suivant (T4).

Si RND1 vaut zéro, on commence par $T1(TC_0)$, $T2(TC_0)$, $T3(TC_0)$ et on finit par $T1(TC_1)$, $T2(TC_0)$, $T3(TC_0)$.

Arrivé à la fin du tour T13, on sauvegarde les paramètres fournis par ce tour, L13, R13, dans la mémoire temporaire CONTEXT0, et on procède pour les

tours restants T14, T15 et T16 de façon similaire aux premiers tours.

Dans tous les cas, il faut que le nombre d'instructions soit exactement le même quel que soit le chemin de calcul. C'est pour cela notamment que dans l'exemple d'application décrit, on prévoit de sauvegarder aussi les valeurs fausses (L3', R3' ou L16', R16') dans la zone mémoire temporaire CONTEXT2.

En effet si une différence quelconque existait entre les deux chemins possibles, il y aurait alors une possibilité d'attaque DPA fructueuse.

Le procédé de contre-mesure selon l'invention n'est pas limité à l'exemple particulier de réalisation décrit en référence à l'algorithme DES. Il s'applique à tout algorithme de cryptographie à clé secrète. De manière générale, pour toute mise en oeuvre d'un algorithme comprenant l'utilisation de premiers moyens pour fournir une donnée de sortie à partir d'une donnée d'entrée, la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques, le procédé de contre-mesure selon l'invention comprend l'utilisation d'autres moyens, en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

L'utilisation des différents moyens , c'est à dire des premiers moyens et des autres moyens, est gérée selon une loi statistique de probabilité un demi.

Les autres moyens peuvent comprendre plusieurs moyens différents. Ils sont tels qu'à l'une ou à l'autre des données d'entrée et de sortie des premiers moyens, ils font correspondre la donnée complémentée.

Dans l'exemple d'un mode d'application du procédé de contre-mesure au DES plus particulièrement décrit, les premiers moyens consistent en la première table de constantes TC_0. Les autres moyens consistent, en début de DES, dans la deuxième table de constantes TC_1. En

fin de DES, ils consistent en deux tables de constantes différentes, TC_1 et TC_2 dans l'exemple.

Pour appliquer le procédé de contre-mesure selon l'invention à un algorithme de cryptographie à clé secrète donné, il faut donc d'abord déterminer toutes les données de cet algorithme qui peuvent être prédites et toutes les instructions critiques au sens de l'attaque DPA manipulant ces données ou des données dérivées. Il faut ensuite identifier dans l'algorithme des premiers moyens et des autres moyens au sens de l'invention, en sorte que toutes les données manipulées par les instructions critiques soient imprédictibles. Les premiers moyens sont, pour l'algorithme DES, la table de constantes TC_0. Les autres moyens sont dans l'exemple, d'autres tables de constantes. Ces moyens peuvent être des opérations différentes pour d'autres algorithmes. Pour un même algorithme, ces moyens peuvent consister en des opérations différentes selon les instructions critiques identifiées.

Le composant électronique 1 mettant en oeuvre un tel procédé de contre-mesure dans un algorithme de cryptographie à clé secrète comprend typiquement, comme représenté sur la figure 12, un microprocesseur µP, une mémoire programme 2 et une mémoire de travail 3. Pour pouvoir gérer l'utilisation des différents moyens selon l'invention, qui sont, dans l'exemple décrit, les différentes tables de constantes mémorisées en mémoire programme, des moyens 4 de génération d'une valeur aléatoire entre 0 et 1, sont prévus qui, si on se reporte à la figure 11, fourniront la valeur de RND1 à chaque exécution du DES. Un tel composant peut tout particulièrement être utilisé dans une carte à puce CP, pour améliorer leur inviolabilité.

REVENDICATIONS

1. Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (K), la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers moyens (TC_0) pour fournir une donnée de sortie (S) à partir d'une donnée d'entrée (E), la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques, caractérisé en ce que le procédé de contre-mesure prévoit l'utilisation d'autres moyens (TC_1), en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

2. Procédé de contre-mesure selon la revendication 1, caractérisé en ce que l'utilisation des différents moyens (TC_0, TC_1) est gérée par une loi statistique de probabilité un demi.

3. Procédé de contre-mesure selon la revendication 2, la mise en oeuvre de l'algorithme comprenant seize tours de calcul (T1, ...,T16), caractérisé en ce qu'il comprend l'exécution d'une première séquence (SEQA) et d'une deuxième séquence (SEQB) formées des trois premiers tours au moins (T1, T2, T3), l'ordre d'exécution des séquences étant fonction de la loi statistique de probabilité un demi, la première séquence (SEQA) utilisant les premiers moyens (TC_0) dans chaque tour, la deuxième séquence (SEQB) utilisant les autres moyens (TC_1) dans le premier tour (T1) au moins.

4. Procédé de contre-mesure selon la revendication 3, caractérisé en ce que la première et la deuxième

séquences sont formées chacune des trois premiers tours (T1, T2, T3).

5. Procédé de contre-mesure selon la revendication 3 ou 4, caractérisé en ce que les autres moyens consistent en des deuxièmes moyens (TC_1) tels que pour une même donnée d'entrée (E), ils fournissent en sortie le complément (/S) de la donnée de sortie (S) des premiers moyens (TC_0).

6. Procédé de contre-mesure selon la revendication 2, la mise en oeuvre de l'algorithme comprenant seize tours de calcul (T1, ...,T16), caractérisé en ce qu'il comprend l'exécution d'une première séquence (SEQA') et d'une deuxième séquence (SEQB') formées chacune des trois derniers tours (T14, T15, T16) au moins, l'ordre d'exécution des séquences étant fonction de la loi statistique de probabilité un demi, la première séquence (SEQA') utilisant les premiers moyens (TC_0) dans chaque tour, la deuxième séquence (SEQB') utilisant les autres moyens (TC_1, TC_2).

7. Procédé de contre-mesure selon la revendication 6, caractérisé en ce que la première et la deuxième séquences sont formées chacune des trois derniers tours, et en ce que les autres moyens utilisés dans la deuxième séquence comprennent des deuxièmes moyens (TC_1) et des troisièmes moyens (TC_2).

8. Procédé de contre-mesure selon la revendication 6 ou 7, caractérisé en ce que les deuxièmes moyens (TC_1) sont tels que pour une même donnée d'entrée (E), ils fournissent en sortie le complément (/S) de la donnée de sortie (S) des premiers moyens (TC_0) et en ce que ces deuxièmes moyens sont utilisés dans la deuxième séquence (SEQB') pour le quatorzième tour (T14).

9. Procédé de contre-mesure selon la revendication 8, caractérisé en ce que les troisièmes moyens (TC_2) sont tels que pour le complément de la donnée d'entrée (E), ils fournissent en sortie le complément (/S) de la donnée de sortie (S) des premiers moyens (TC_0) et sont utilisés dans la deuxième séquence, pour le quinzième tour et le seizième tour (T15, T16).

10. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens sont des tables de constantes.

11. Composant électronique mettant en oeuvre le procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens (TC_0, TC_1, TC_2) pour fournir une donnée de sortie à partir d'une donnée d'entrée sont fixés en mémoire programme du dit composant et en ce qu'il comprend des moyens de génération d'une valeur aléatoire (RND1) à 0 ou à 1 pour gérer l'utilisation des dits différents moyens.

12. Carte à puce comprenant un composant électronique selon la revendication 11.

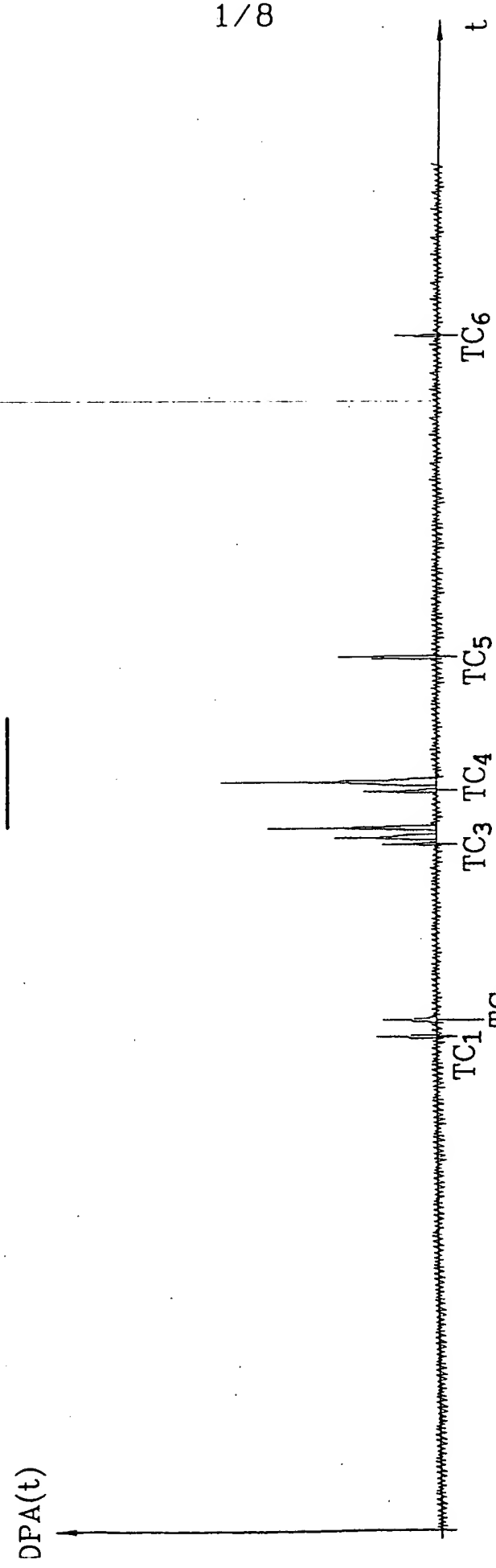


FIG.1

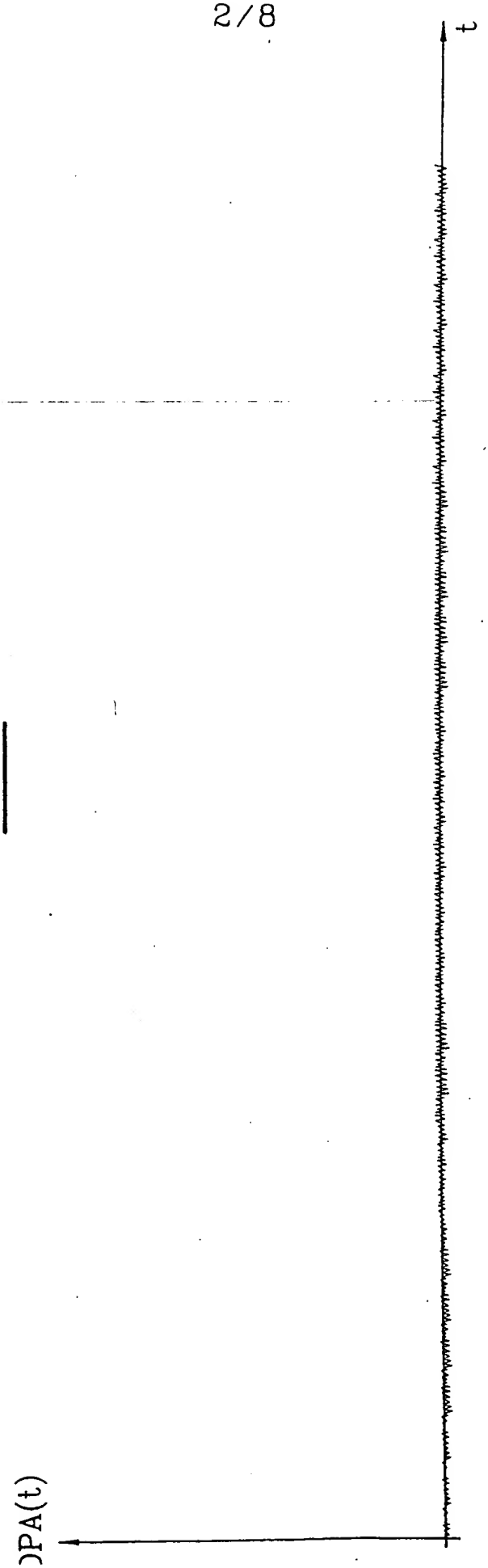


FIG.2

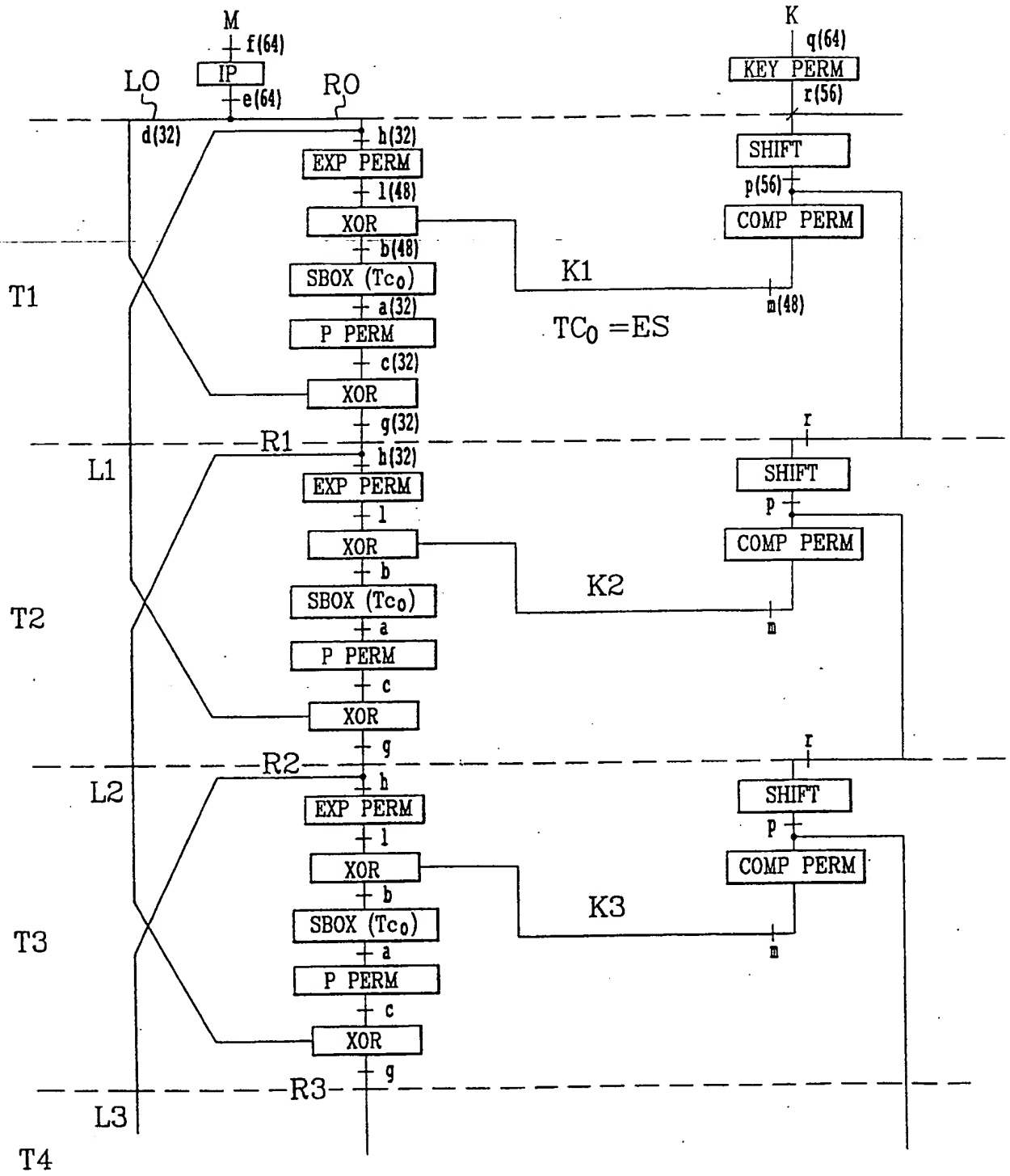

M
f(64)
IP
e(64)
LO
RO
d(32)
h(32)
EXP PERM
l(48)
XOR
b(48)
SBOX (Tc0)
a(32)
P PERM
c(32)
XOR
g(32)
K
q(64)
KEY PERM
r(56)
SHIFT
p(56)
COMP PERM
K1
m(48)
TC0 =ES
T1
R1
L1
T2
K2
R2
L2
T3
K3
R3
L3
T4

FIG.3

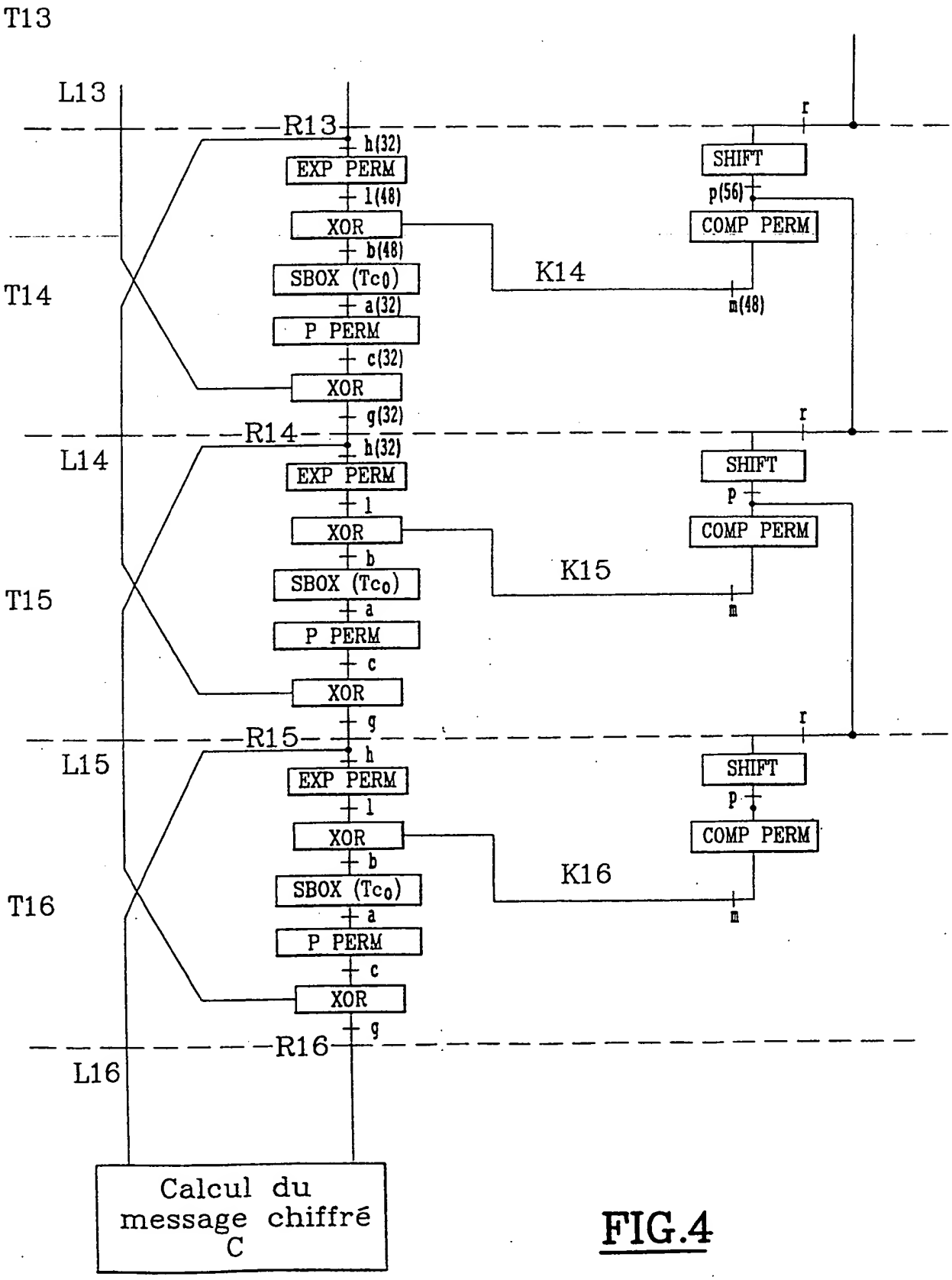

T13
L13
R13
h(32)
EXP PERM
l(48)
XOR
b(48)
SBOX (Tc0)
a(32)
P PERM
c(32)
XOR
g(32)
r
SHIFT
p(56)
COMP PERM
K14
m(48)
T14
R14
L14
h(32)
EXP PERM
l
XOR
b
SBOX (Tc0)
a
P PERM
c
XOR
g
r
SHIFT
p
COMP PERM
K15
m
T15
R15
L15
h
EXP PERM
l
XOR
b
SBOX (Tc0)
a
P PERM
c
XOR
g
r
SHIFT
p
COMP PERM
K16
m
T16
R16
L16
Calcul du message chiffré C

FIG.4

FIG.5

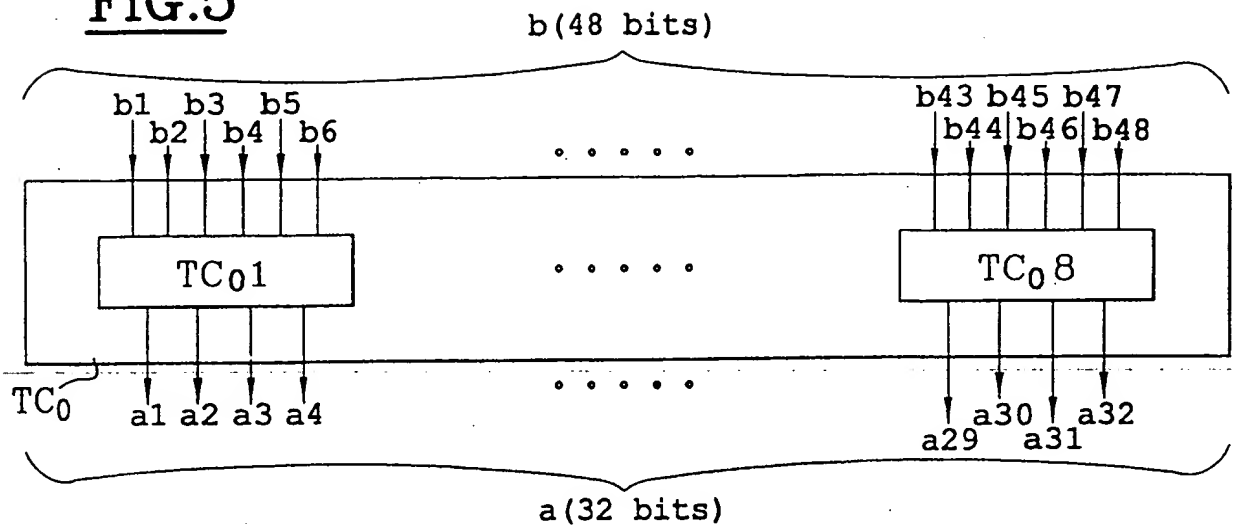


FIG.6

TC0 1

E1=b1b2b3b4b5b6	S1=a1a2a3a4
000000	1101
000001	0101
⋮	⋮
111111	1010

FIG.9

TC1 1

E1=b1b2b3b4b5b6	/S1=$\overline{a1a2a3a4}$
000000	0010
000001	1010
⋮	⋮
111111	0101

FIG.10

TC2 1

/E1=$\overline{b1b2b3b4b5b6}$	/S1=$\overline{a1a2a3a4}$
000000	0101
⋮	⋮
111110	1010
111111	0010

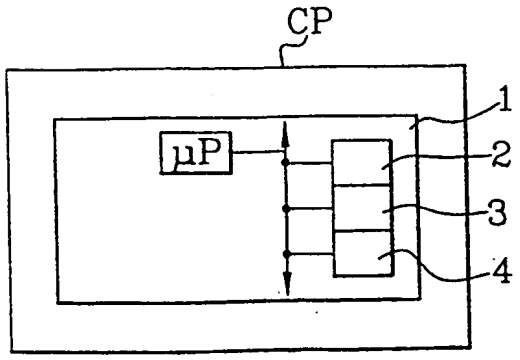


FIG.12

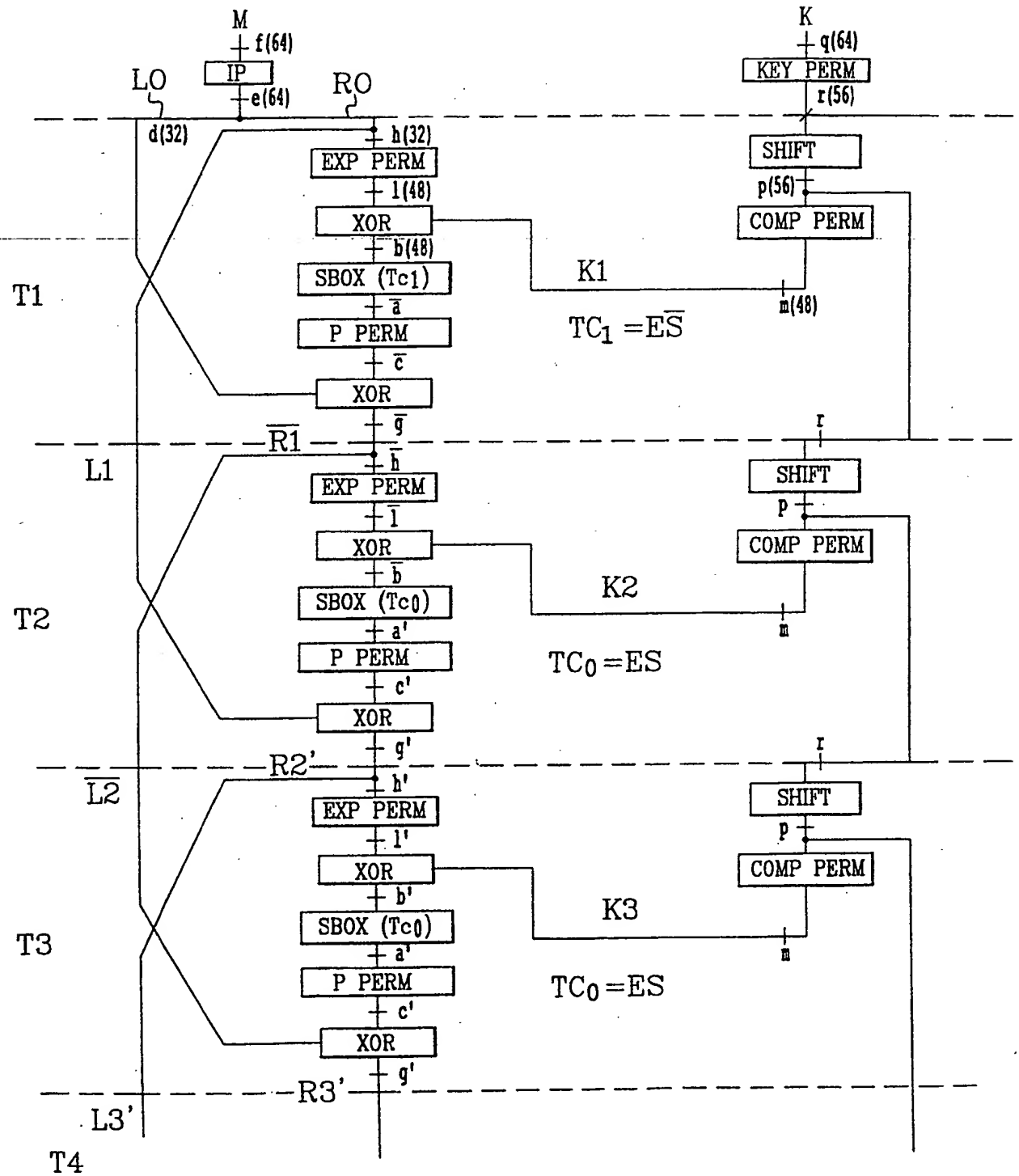

M
f(64)
IP
e(64)
LO
RO
d(32)
h(32)
EXP PERM
l(48)
XOR
b(48)
SBOX (Tc1)
a
P PERM
c
XOR
g
R1
T1
K
q(64)
KEY PERM
r(56)
SHIFT
p(56)
COMP PERM
K1
m(48)
TC1 =ES
L1
T2
SBOX (Tc0)
K2
TC0 =ES
R2'
L2
T3
K3
R3'
L3'
T4

FIG.7

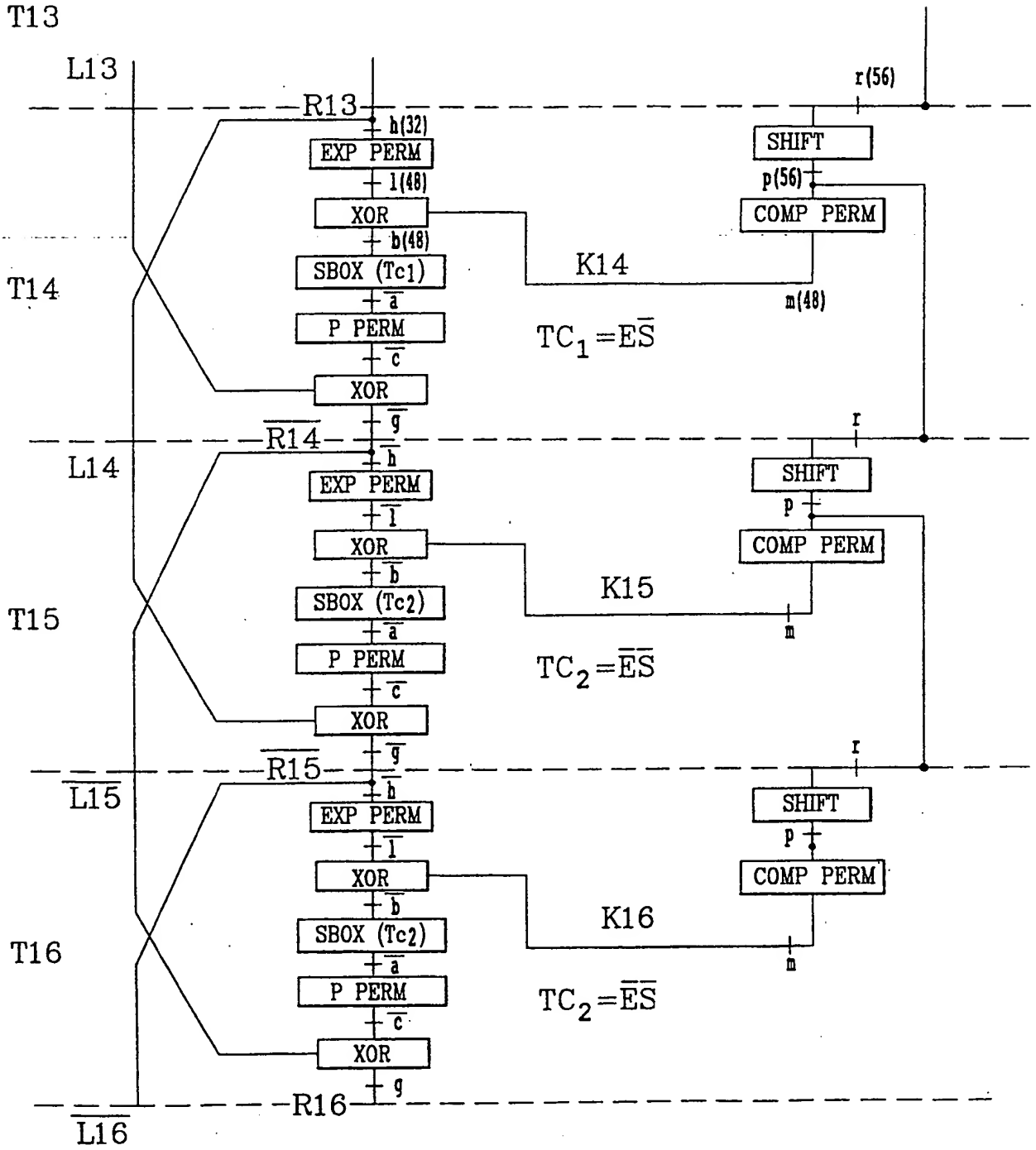

T13
L13
R13
h(32)
EXP PERM
l(48)
XOR
b(48)
SBOX (Tc1)
a
P PERM
c
XOR
g
r(56)
SHIFT
p(56)
COMP PERM
K14
m(48)
TC1=ES
T14
R14
L14
h
EXP PERM
l
XOR
b
SBOX (Tc2)
a
P PERM
c
XOR
g
r
SHIFT
p
COMP PERM
K15
m
TC2=ES
T15
R15
L15
h
EXP PERM
l
XOR
b
SBOX (Tc2)
a
P PERM
c
XOR
g
r
SHIFT
p
COMP PERM
K16
m
TC2=ES
T16
R16
L16

FIG.8

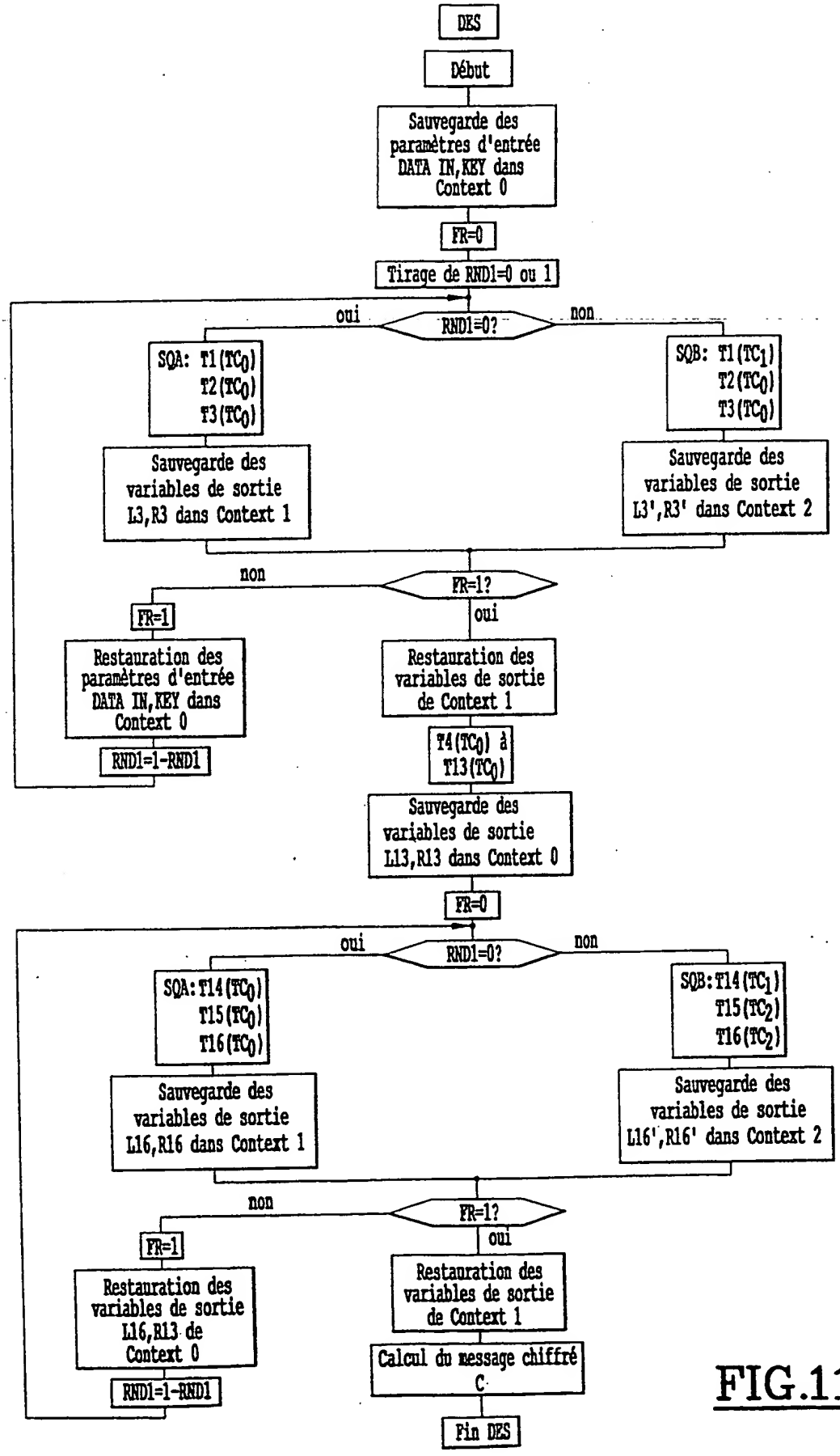

DES
Début
Sauvegarde des paramètres d'entrée DATA IN,KEY dans Context 0
FR=0
Tirage de RND1=0 ou 1
RND1=0?
oui
non
SQA: T1(TC0) T2(TC0) T3(TC0)
SQB: T1(TC1) T2(TC0) T3(TC0)
Sauvegarde des variables de sortie L3,R3 dans Context 1
Sauvegarde des variables de sortie L3',R3' dans Context 2
FR=1?
non
oui
FR=1
Restauration des paramètres d'entrée DATA IN,KEY dans Context 0
RND1=1-RND1
Restauration des variables de sortie de Context 1
T4(TC0) à T13(TC0)
Sauvegarde des variables de sortie L13,R13 dans Context 0
FR=0
RND1=0?
oui
non
SQA: T14(TC0) T15(TC0) T16(TC0)
SQB: T14(TC1) T15(TC2) T16(TC2)
Sauvegarde des variables de sortie L16,R16 dans Context 1
Sauvegarde des variables de sortie L16',R16' dans Context 2
FR=1?
non
oui
FR=1
Restauration des variables de sortie L16,R13 de Context 0
RND1=1-RND1
Restauration des variables de sortie de Context 1
Calcul du message chiffré C
Fin DES

FIG.11

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 99/02172

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 November 1997 (1997-11-03), pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS abstract column 1, line 13 - line 29 column 2, line 6 - line 18 column 3, line 1 -column 5, line 1 --- -/--	1,2,10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 2000	18/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

3

Form PCT/ISA/210 (second sheet) (July 1992)

Inter al Application No
PCT/FR 99/02172

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category ³	Citation of document, with indication, where appropnate, of the relevant passages	Relevant to claim No.
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THECONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 July 1994 (1994-07-01), pages 85-90, XP000460342 the whole document	1
A	FR 2 672 402 A (GEMPLUS CARD INT) 7 August 1992 (1992-08-07) abstract page 1, line 4 - line 12 page 3, line 19 - line 23 figure 1 claim 1	11,12

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2672402 A	07-08-1992	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

n. internationale No
PCT/FR 99/02172

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997 (1997-11-03), pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS abrégé colonne 1, ligne 13 - ligne 29 colonne 2, ligne 6 - ligne 18 colonne 3, ligne 1 -colonne 5, ligne 1 --- -/--	1,2,10

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories speciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 janvier 2000	18/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

3

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THECONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 juillet 1994 (1994-07-01), pages 85-90, XP000460342 le document en entier	1
A	FR 2 672 402 A (GEMPLUS CARD INT) 7 août 1992 (1992-08-07) abrégé page 1, ligne 4 - ligne 12 page 3, ligne 19 - ligne 23 figure 1 revendication 1	11,12

Renseignements relatifs aux membres de familles de brevets

Internationale No
PCT/FR 99/02172

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2672402 A	07-08-1992	AUCUN	